3/PRTS

DEVICES FOR HIDING THE OPERATIONS PERFORMED IN A MICROPROCESSOR CARD

Ins. a'

The invention relates to microprocessor cards and, in such cards, different devices for hiding the operations performed in the card for the purpose of improving security against fraudulent intrusions.

Chip cards are divided into several categories, namely:

- simple-memory cards,
- memory cards known as smart cards, and
- microprocessor cards.

A simple-memory card makes it possible to perform read and write operations freely in the electrically erasable read only memory area. Such a card is inexpensive but does not offer sufficient security so that it is being used less and less.

a

A smart memory card notably improves the security of the read/write operations by enabling them

only when certain conditions implemented in hard-wired form are fulfilled.

A card in the third category contains a microprocessor capable of executing programs recorded in a memory and thus making calculations with secret data inaccessible to the world external to the card. Thus a key recorded in the memory can serve to validate an electronic transaction such as a purchase or a door opening without having to be manipulated outside the card.

Unfortunately, certain microprocessors have current consumptions which depend on the calculations made inside the card. Thus a cryptographic calculation comprising a calculation tree which depends on the digits of the key used will have different current consumption footprints according to the value of the key used. As a result a fraudster could correlate the current consumption footprint of the key used and thus go back to the value of the key.

To prevent this correlation, a usual countermeasure consists of programming the cryptographic algorithm so that, whatever the value of the key, the algorithm will always pass through the same calculation steps.

Many so-called "byte oriented" algorithms lend themselves well to this program mode, but others pose a few technical problems which are surmountable only at the cost of a less optimal calculatory performance.

Summary of the Invention

The purpose of the present invention is therefore to use, in microprocessor cards, devices for hiding the

operations performed whilst permitting the programmer the free choice of the programming rules, whether or not they are of the "byte oriented" type.

This purpose is achieved by modifying or scrambling the consumption of the card so that its footprint is independent of the calculations made.

This modification or scrambling of the footprint can be obtained by adding a device to the card which modifies the current consumption.

In a first example embodiment, this device consumes electrical power in an irregular or random manner, which is added to that of the normal consumption.

In a second example embodiment, this device achieves a mean consumption by effecting, for example, an integration of the current consumed.

In a third example embodiment, this device triggers the microprocessor memory erasure or programming circuit which consumes power in a chaotic manner, power which masks the consumption due to the operations performed by the microprocessor during the programming or erasure of the memory.

Brief Description of the Drawings

Other characteristics and advantages of the present invention will emerge from a reading of the following description of particular example embodiments, the said description being given in relation to the accompanying drawings, in which:

- Figure 1 is a functional diagram of a first example embodiment of the invention,

- Figure 2 is a functional diagram of a second example embodiment of the invention, and

- Figure 3 is a functional diagram of a third example embodiment of the invention.

Detailed Description

In the figures, which each show schematically different means for implementing the invention, the electronic chip 10 containing the microprocessor of the card comprises a central unit 12 and at least one memory 14, for example of the type known by the English acronym EEPROM, standing for Electrically Erasable Programmable Read Only Memory. This electronic chip has several input and/or output terminals 16_1 to 16_8, one of which, referenced 16_1, is connected to an electrical circuit 18 supplying voltage V_{CC} whilst the one referenced 16_5 is connected to ground.

The supply circuit 18 supplies the different elements of the electronic chip 10 with a current I_{out} and, notably, the memory 14 and the central unit 12. This current I_{out} varies according to the operations performed by the central unit and the memory and therefore reflects the cryptographic calculations, which could make it possible to determine the key thereof.

So that this current I_{out} no longer reflects the operations performed, the invention proposes to modify it by means of a device 20 or 30, disposed in the chip 10 and connected, for example, to the input terminal 16_1.

The invention proposes to modify the current in two different ways. A first by ensuring that the

device 20 (Figure 1) consumes current in a random or at the very least irregular manner, random additional consumption which, added to the normal current consumption I_{in}, makes the value I_{out} random.

The second way consists in averaging the value of I_{in}, which does not make it possible to detect the variations in I_{in} due to the operations performed.

In the first case, the device 20 can be produced by means of resistors 30, in fact transistors, which are powered or not according to the random signals supplied by a generator 28. The currents flowing in the powered resistors increase, modifying the total current value and hiding the current due to the cryptographic calculations.

In the second case, the average of the current I_{in} is obtained by an integrator which "smooths" the variations in the current I_{in} so as to erase them.

According to the invention, several devices 20 or 30, referenced 20_1 and 30_1, can be connected to different points on the electronic chip, for example to the power supply conductor of the central unit (reference 22). In addition, these devices 20, 20_1, 30 and 30_1 can be connected or not, depending on whether the operations are to be protected or not, the connections being made under the control of signals supplied by the central unit 12 (broken lines).

The invention proposes a third way of scrambling the value of I_{out} whilst performing operations to be protected, such as cryptographic calculations, during certain phases of the operations of programming or

erasing the memory 14, these operations being under the control of the central unit 12.

This third way is based on the use of a memory 14 of the EEPROM type which has auto-writing capability.

In a normal operating mode, the microprocessor activates a programming circuit 24 of the memory 14 according to the following steps:

1 – activation of the charge pump,

2 – presentation, on the data bus, of the data item to be written,

3 – presentation on the address bus of the writing address,

4 – initiation of the programming,

5 – waiting during the programming time,

6 – stopping the programming,

7 – stopping the charge pump.

Since the programming of an EEPROM cell makes it necessary to inject electrical charges into the programmed cell, steps 4, 5 and 6 are accompanied by an over-consumption of current of chaotic appearance which depends essentially on the value of V_{CC}, the address, the programmed value and the temperature of the component.

In order to mask the current consumption footprint of a cryptographic calculation for example, the invention proposes to use the chaotic consumption of steps 4, 5 and 6 by performing the cryptographic calculation during step 5 for a period of a few microseconds.

To do this, the cryptographic calculation is performed according to the following steps:

1 - starting the charge pump,

2 - presentation of a random data item on the data bus,

3 - presentation of a writing address on the address bus,

4 - initiation of the programming,

5 - effecting the cryptographic calculation,

6 - stopping the programming,

7 - stopping the charge pump.

Through these steps, the footprint of the current consumption due to the cryptographic calculation of step 5 is masked by the writing of the random data item in a given part 26 of the EEPROM memory reserved for this function.

Instead of a cryptographic calculation, step 5 can consist of any operation to be protected vis-à-vis the outside.

In addition, instead of performing these operations to be protected during a writing in the memory 14, they can be done during an erasure of the memory 14.